ISSN:0975-9646

Novel Intrusion Detection in MANETs based on Trust

Devendra Singh[1], S. S. Bedi[2]

[1]*Computer Science and Engineering Department, IFTM University, Moradabad, India*[1]
[2]*Computer Science and Engineering Department, MJP Rohilkhand University, Bareilly, India2*

Abstract— **Mobile Ad hoc Network is comprised of several mobile nodes without any centralized infrastructure. MANETs are lack of boundaries due to wireless communication medium. Due to the absence of centralized infrastructure, changing topology and distributed nature, MANETs is prone to several security threats and intruders. Thus, it is necessary to safeguard the network from malicious nodes. Thus to overcome with this security issue we need to develop a robust, flexible intrusion detection system. This paper aims at detecting the malicious nodes by proposing an Intrusion Detection System (IDS). We plan to employ KDD'99 dataset and the features are planned to get selected by mutual information and information gain ratio. A trust based multi-class Extreme Learning Machine (ELM) is planned to be incorporated for effective classification of malicious nodes. The expected outcome of the system will be effective as the system considers trust value of nodes. The performance metrics that will be used to check the performance of the system are misclassification rate, detection accuracy, execution time and false alarm rate under different scenarios. Thus our work provides novel way of Intrusion Detection.**

Keywords— **Intrusion Detection System, MANETs, Trust, Anomaly Detection, Malicious node.**

I. INTRODUCTION

MANET is comprised of several mobile nodes in the absence of centralized infrastructure. As there is no underlying infrastructure, the participating nodes of MANET act both as the host and the router. AdHoc networks are used to rapid deployment of a network on the urgent temporary basis or for specific purposes such as disaster recovery, military battle field, and small offices of universities. In MANET, a node can join in network or leave the network at any time. .MANET is prone to several security threats due to the mobile nature of nodes [1]. The issue of security is of paramount concern in MANETs. There are some security issues in MANETs such as unauthorized access, attacks within the network and outside the network or any unwanted activities in the network. Intrusion Detection System is a technique to detect and supervise the network and prevent the network from inside and outside attacks by collecting information about the network traffic and nodes behaviors. Thus, deployment of an Intrusion Detection System (IDS) is necessary to safeguard the network. To implement IDS in MANETs, we need to focus on the weaknesses of MANETs such as it does not create new weakness to network, takes little resources, power, bandwidth, run continuously, fair and reliable. To achieve all these goals our Intrusion Detection System (IDS) provides the security and at the same time consumes very little energy.

There are two different types of attacks that can happen to a network. They are active attacks and passive attacks [2]. Active attacks are attacks that alter the content of the data. Single intruder can perform intrusive activity such as modifying, injecting, forging, fabricating, dropping data or routing packets, resulting in disruption to the network and others can be caused by a sequence of activities by colluding intruders. These attacks can degrade the network performance significantly or bring down the network, such as denial of service. Passive attacks usually listen to the data exchange between nodes but attempts to seek some valuable information through network routing traffic analysis. By listening network traffic, attackers can get the critical information about the network or the places of nodes through network topology and the nodes identity. Some passive attacks are eavesdropping, location disclosure, traffic analysis. These attacks may be the root cause for network traffic, incorrect service or the complete network may get shattered.

An IDS has three different subsystems [3] and they are data aggregation, detect any misbehaviour and respond to the other nodes about detected misbehaviour. Firstly, collection of data or monitoring is done through all or selected nodes in the networks at packet level, user level, network level and application logs. Secondly, detection processes is done through some detection engines/techniques viz. anomaly, misuse and specification based. Lastly, third one is response process in which detected node sends an alert message to all the benign nodes. An IDS can follow stand alone, hierarchical or a cooperative architecture [4]. In the stand alone flavour of IDS, every node locally executes IDS and thus the response will be local. This type of detection system can detect the intruder or attacks locally because nodes are not sharing data with other nodes. The main drawback of this is the reduced detection accuracy. The hierarchical architecture relies on the cluster head. In this approach, the network is divided into several clusters and a cluster head is chosen based on some characteristic features. It is something like a virtual centralized monitoring system. Cluster head is responsible to detect attacks. Cluster members may have light detection mechanism to save its resources. The merit of this approach is the effective utilization of restricted energy and the demerit is that it has to cope up with the mobility. Due to high mobility system needs new cluster head, when existing cluster head may out of reach. Thus, it is more suitable for multilayer network infrastructure than a flat network infrastructure. In the cooperative IDS, every node collects the audit data and shares it to other nodes and IDS deploys locally. However, they coordinate with the other participating nodes, to take any decision and thus alarm other nodes about the malicious node(s). This system gives law false alarm and high accuracy. In this paper we have proposed a novel intrusion detection system calculating trust of nodes after classification. The rest of the paper is organized as follows. The literature survey is presented in section II. Section III gives the proposed IDS architecture and working principles. Finally, section IV concludes the proposed work and planning of possible future works.

II. Literature SURVEY

This section summarizes the most prominent IDS for MANETs. A lot of works have been done on security of MANETs, intrusion prevention as well as intrusion detection but few papers have been considered for this work.

Zone-Based Intrusion Detection for Mobile Ad Hoc Networks [5]

Bo Sun at el. in present a non-overlapping Zone-Based Intrusion Detection System (ZBIDS) that fits the requirement of MANETs. They present details of constructing the Markov Chain based local anomaly detection model, including feature extraction, data pre-process, detection engine construction, and parameter tuning. The whole network is divided into non- overlapping zones. There are two categories of nodes in ZBIDS, if one node has a physical connection to a node in a different zone; this node is called a gateway node. Otherwise, it is called an intra-zone node. Only gateway nodes can generate alarms. They collect the local alerts broadcast from the intra-zone nodes and perform aggregation and correlation tasks to suppress many falsified alerts. For avoid of the single point of failure, if exist more than one gateway node in a single zone, all of which perform the alert aggregation task simultaneously.

The functionality of Local Aggregation and Correlation Engine (LACE) is to locally aggregate and correlate the detection results of detection engines. Global Aggregation and Correlation Engine (GACE) in gateway nodes is to aggregate and correlate the detection results from local nodes in order to make final decisions. They can also cooperate with neighbouring gateway nodes to further exchange information. After an attack is identified, based on different attack types, the Intrusion Response Module (IRM) could take corresponding measures, such as identifying the intruders, reinitiating the communication channels, and excluding the compromised nodes from the networks.

Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms [6][7]

Mitrokotsa at el. In design and evaluate of intrusion detection models for MANETs using supervised classification algorithms. They adopt the IDS architecture composed of multiple local IDS agents that are responsible for detecting possible intrusions locally.

They used MultiLayer Perception (MLP), the Linear model, the Gaussian Mixture model (GMM), the Naive Bayes model and the SVM model for classification. All these models require labelled training data for their creation. The IDS architecture they adopt is composed of multiple local IDS agents that are responsible for detecting possible intrusions locally. The collection of all the independent IDS agents forms the IDS system for the MANET. Each local IDS agent is composed of the following components:

Data Collector: is responsible for selecting local audit data and activity logs. Intrusion Detection Engine: is responsible for detecting local intrusions using local audit data. The local intrusion detection is performed using a classification algorithm. Response Engine: If an intrusion is detected by the Detection.

A game-theoretic intrusion detection model for mobile ad hoc networks [8]

Hadi Otrok at el. in addresses the problem of increasing the effectiveness of an intrusion detection system (IDS) for a cluster of nodes in ad hoc networks. To reduce the performance overhead of the IDS, a leader node is usually elected to handle the intrusion detection service on behalf of the whole cluster. To increase the effectiveness of IDS in MANET, they propose a unified framework that is able to: (1) Balance the resource consumption among all the nodes and thus increase the overall lifetime of a cluster by electing truthfully and efficiently the most cost-efficient node known as leader- IDS. A mechanism is designed using Vickrey, Clarke, and Groves (VCG) to achieve the desired goal. (2) Catch and punish a misbehaving leader through checkers that monitor the behaviour of the leader. A cooperative game-theoretic model is proposed to analyze the interaction among checkers to reduce the false-positive rate. A multi-stage catch mechanism is also introduced to reduce the performance overhead of checkers. (3) Maximize the probability of detection for an elected leader to effectively execute the detection service. This is achieved by formulating a zero-sum non-cooperative game between the leader and intruder. We solve the game by finding the Bayesian Nash Equilibrium where the leader's optimal detection strategy is determined. Finally, empirical results are provided to support our solutions.

A Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm [9]

In this proposed algorithm the researcher's aims to utilize one of the danger theory intrusion detection algorithms, namely, the dendritic cell algorithm (DCA) to detect the sleep deprivation attack over MANET. DCA is plugged in a proposed mobile dendritic cell algorithm called MDCA, which is represented through a proposed MDCA architecture. They tried to each node in MANET should protect itself from danger locally without using mobile agents.

The innate subsystem and the adaptive subsystem are two main component of MDCA. The proposed algorithm designed by them is as follow, at the beginning, the algorithm verifies each entered packet's ID in the memory. If that packet ID found in the detected list, this means it comes from an attacker detected before, the algorithm rejects the packet directly, deletes its information from the routing table and sends an alarm message for the second time for that packet ID. Else if the packet ID is found in the alarmed list, this means the packet comes from an attacker detected by another node so it is rejected directly, deleted from the routing table but without sending alarm again. Else, the packet must be analyzed by the packet analyzer. The packet analyzer extracts the required antigens from the routing table and generates the signals from the routing table, the availability of the bandwidth, and the power consumption rate. After that, the packet analyzer stores the antigens and signals in the antigens and signals stores respectively.

BeeID: Intrusion Detection in AODV-based MANETs Using Artificial Bee Colony and Negative Selection Algorithms [11]

In the reference the researchers present a dynamic hybrid approach based on the artificial bee colony (ABC) and negative selection (NS) algorithms, called BeeID, for intrusion detection in AODV-based MANETs. The approach consists of three phases: training, detection, and updating. In the training phase, a niching artificial bee colony algorithm, called Niche NABC, runs a negative selection algorithm multiple times to generate a set of mature negative detectors to cover the nonself space. In the detection phase, mature negative detectors are used to discriminate between normal and malicious network activities. In the updating phase, the set of mature negative detectors is updated by one of two methods of partial updating or total updating. We use the Monte Carlo integration to estimate the amount of the nonself space covered by negative detectors and to determine when the total updating should be done.

Most of the authors are published paper on the survey of literature [10][13]. This paper aims to find the effective intrusion detection system in MANET. None of the above works present a technique to measure the effectiveness of the system.

III. Proposed Work

This paper aims at detecting the malicious nodes by proposing an Intrusion Detection System (IDS). We plan to employ KDD'99 dataset and the features are planned to get selected by information gain and gain ratio. A trust based multi-class Extreme Learning Machine (ELM) is planned to be incorporated for effective classification of malicious nodes. The expected outcome of the system will be effective as the system considers trust value of nodes. The performance metrics that will be used to check the performance of the system are misclassification rate, detection accuracy, execution time and false alarm rate under different scenarios.

A. Overall Architecture Details

The overall architecture of the proposed IDS is given in figure 1. This system consists of different modules and they are user interface, pre-processing, classification and final decision.

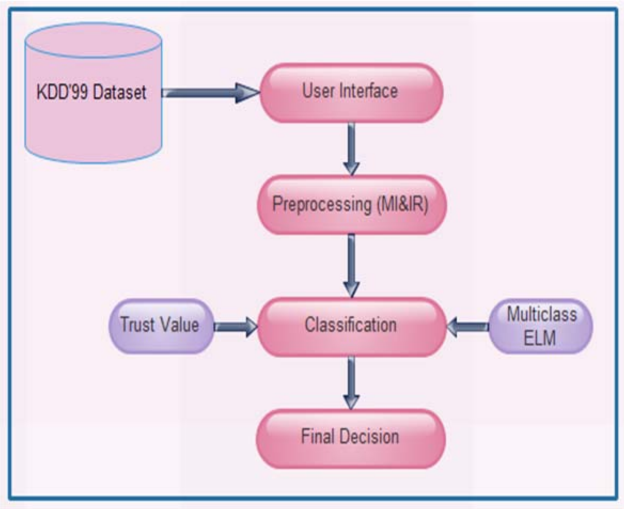

Fig.1 Overall achitecture of proposed IDS

1) User Interface

User interface is the interface through which the user can interact with the system. Network data are monitored for a period of time. Data gathering or audit data are collected through this phase. All the audit information passed through the next pre-processing module.

2) Pre-processing

Pre-processing is the phase in which the data is pre-processed by selecting necessary features alone. This is planned to get achieved by mutual information and information gain ratio. Feature selection is the most important task such that necessary and essential features alone are considered. It makes sense that appropriate features alone are selected and make use of in the forthcoming phases. In case, if the inappropriate features are maintained, processing time will be prolonged. Initially, the mutual information of the features is calculated and will be given a label. This is followed by the selection of features with respect to the mutual information. This process continues until the necessary set of features is figured out. Information gain examines the features by calculating the information gain with regard to the label and the gain ratio normalizes the information gain, such that the most appropriate features are selected.

Information Gain takes all the features into account with regard to the class. Entropy plays a vital role here, which is the amount of information relevant to the source. The information gain is calculated by

$$I\_Gain=EI\ (f1,\ f2\ldots\ldots..fn) - E\ (F)$$

Where I_Gain is the Information Gain, EI is the Expected Information, f1, f2…fn are the feature sets and E (F) is the entropy of the feature. However, this tends to select features with greater values.

Information Gain Ratio normalizes the information gain by a value and can be given by

$$I\_G= -\sum_{1}^{m}\left(\frac{|c1|}{|c|}\right) log_2\left(\frac{|c1|}{|c|}\right)$$

The above presented equation divides the feature set into several parts and the gain ratio can be calculated by

$$I\_G\_F = \frac{I\_Gain}{I\_G}$$

3) *Classification Phase*

This phase aims at classifying the malicious nodes from the normal nodes. There are so many classifiers available to classify these types of problems such as Support Vector Machines, Naive baysian filter, PCA which are used by the researchers []. Here we are using multi class Extreme Learning Machines which proved better than all these classifiers in []. Initially, the multi class ELM is trained with the system for some time. Next in its testing phase gives detected nodes. This can be achieved by two different ideas and they are trust based mechanism and multi-class ELM.

Input:
TrainingData_File - Filename of training data set
TestingData_File - Filename of testing data set
Elm_Type - ELM as functional approximators or classifiers 1 for (both binary and multi-classes) classification
Regularization_coefficient - Regularization coefficient C
Kernel_type - Type of kernels:
'RBF_kernel' for RBF Kernel
'lin_kernel' for Linear Kernel
'poly_kernel' for Polynomial Kernel
'wav_kernel' for Wavelet Kernel
kernel_para - A number or vector of Kernel Parameters
Output:
TrainingTime - CPU Time (seconds) spent on training ELM
TestingTime - CPU Time (seconds) spent on predicting ALL testing data
TrainingAccuracy - Training accuracy:
RMSE for regression or correct classification rate for classification
TestingAccuracy - Testing accuracy:

The trust value of a node is determined by the forwarding ratio and behavioural constant and energy. The multi-class ELM then classifies between the normal and the malicious node. ELM is employed because of its faster learning potency.

Trust value is very important in the forthcoming phases because this is responsible for calculating the trust about the node. This trust value will be one of the parameter to decide intrusions and used by classifier to classify among the malicious or benign node. The trust value is computed by taking forwarding ratio, behaviour of the node and energy into account. Trust value must be normalized between 0 and 1.

Packet Forwarding Ratio: This is the ratio of the successfully transmitted packets to the actual number of packets passed to the node.

$$PFR = \frac{Successfully\ transmitted\ packets}{Total\ number\ of\ packets} X\ 100$$

With this metric, the actual attitude of the node can be figured out. If the ratio close to 0 nodes is not forwarding the packets and it may be a malicious node but we cannot consider this parameter to declare it malicious because packets can be dropped due to congestion in network.

Behaviour: This parameter is computed by tracking the node for a period of time [0, t], such that the total number of interactions with other nodes and the coordination of the node can be determined. This parameter shows the node's honesty with the parameters PFR and behaviour, a small concept of selfishness is considered.

Energy: The energy of every node will get deteriorated with respect to time. Thus, it is necessary to track the energy level of the node, such that the intended task can be accomplished. A node can achieve any task, only when it has sufficient energy.

By combining all the aforementioned parameters, the trust value is computed by taking average of these three parameters in normalized form for making computation effective.

4) *Decision phase*

In this phase, final decision is declared with the outcome of the classification phase and the step needed to handle the intrusions is known as response system. Response system can be presented as the next phase. However, it is not the scope of IDS. To decide the malicious node there should be some decision authority on the basis of threshold values of trust level. The nodes which are found to be malicious will be blocked. Blocking nodes list will send to all nodes in the network. Thus, the normal nodes will not forward or receive any packets from the nodes of blocked list.

This work categorizes selfish nodes and malicious nodes. A final declaration table will be maintained for the system with respect to the trust value. If the trust value is greater than 90%, then no action is required. If the trust value is greater than 50%, then these nodes may get temporarily blocked, and if the trust value is lesser than 50%, then those nodes will be added to the block list.

IV. Conclusions

In this work, we proposed a novel intrusion detection system based on the trust value of node and classifier. The main advantages of the proposed intrusion detection system are that it does not block the node suddenly due to the threshold values used for permanent block and temporary block of intrusive node. Decision phase will generate a list of permanent and temporary blocking nodes according to the trust level. If temporary blocks node behaves well for some period of time, then they removed from the blocking list. With this blocking policy network remains found effective. Apart from this, a small concern about selfishness of node is also presented. Most advanced ELM classifier is used to train and test the system. The expected outcome of the system will be the effective detection of any intrusion with reduced false alarm rate, misclassification rate and improved detection accuracy. For the future work, practically results of this proposed method and designing efficient algorithms for each phase of the proposed IDS architecture.

REFERENCES

[1] J.N. Al-Karaki; A.E. Kamal: “Routing Techniques in Wireless Sensor Networks: A Survey,” IEEE Wireless Comm., vol. 11, no. 6, pp. 6-28, (2004).

[2] Nadeem, A.; Howarth, M.P., "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks," *Communications Surveys & Tutorials, IEEE* , vol.15, no.4, pp.2027,2045, Fourth Quarter 2013

[3] Sannasi Ganapathy; Kanagasabai Kulothungan; Sannasy Muthurajkumar; Muthusamy Vijayalakshmi; Palanichamy Yogesh; Arputharaj Kannan: "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey", EURASIP Journal on Wireless Communications and Networking, No. 271, pp.1-16, (2013).

[4] Blazevic, L.; Buttyan, L.; Capkun, S.; Giordano, S.; Hubaux, J.-P.; Le Boudec, J.-Y., "Self organization in mobile ad hoc networks: the approach of Terminodes," Communications Magazine, IEEE , vol.39, no.6, pp.166,174, Jun 2001

[5] Sun, Bo, Kui Wu, and Udo W. Pooch. "Zone-based intrusion detection for mobile ad hoc networks." *Int. Journal of Ad Hoc and Sensor Wireless Networks*2.3 (2003): 2003-9.

[6] Mitrokotsa, Aikaterini; Komninos, Nikos; Douligeris, Christos, "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET," *Pervasive Services, IEEE International Conference on* , vol., no., pp.118,127, 15-20 July 2007

[7] Aikaterini Mitrokotsa and Christos Dimitrakakis. 2013. Intrusion detection in MANET using classification algorithms: The effects of cost and model selection. *Ad Hoc Netw.* 11, 1 (January 2013), 226-237.

[8] Hadi Otrok, Noman Mohammed, Lingyu Wang, Mourad Debbabi, and Prabir Bhattacharya. 2008. A game-theoretic intrusion detection model for mobile ad hoc networks. *Comput. Commun.* 31, 4 (March 2008), 708-721.

[9] Maha Abdelhaq. Detecting sleep deprivation attack over MANET using a danger theory –based algorithm. International Journal of New Computer Architectures and their Applications (IJNCAA), 3(1), 2011.

[10] Amiri, E.; Afshar, E.; Naji, H.R.; Ardekani, M.M., "Survey on network access control technology in MANETs," *Innovation Management and Technology Research (ICIMTR), 2012 International Conference on* , vol., no., pp.367,372, 21-22 May 2012

[11] Barani, Fatemeh, and Mahdi Abadi. "BeeID: Intrusion Detection in AODV-based MANETs Using Artificial Bee Colony and Negative Selection Algorithms." *The ISC International Journal of Information Security* 4.1 (2015).

[12] Dang, Nish, and Pooja Mittal. "Cluster based intrusion d etection system for MANETS." *International Journal of Computer Applications & Information Technology* 1.1 (2012).

[13] Devendra Singh and S. S Bedi. Article: A State of an Art Survey of Intrusion Detection System in Mobile Ad-hoc Network. *International Journal of Computer Applications* 82(5):7-12, November 2013.